

CITY OF SAN ANTONIO



Administrative Directive

AD 7.8F Electronic Signatures and Records

Procedural Guidelines

Guidelines to establish electronic signatures and electronic records.

Department/Division

Information Technology Services Department (ITSD) and the Office of the City Clerk

Effective Date

March 15, 2010

Project Manager

John Byers, Chief Information Security Officer (CISO)

Purpose

This directive is jointly issued by the Information Technology Services Department (ITSD) and the Office of the City Clerk for establishing when an electronic signature may replace a written signature and when an electronic record may replace a paper document for official business of the City of San Antonio (COSA). This directive applies to all employees, contractors, vendors, and third-party providers to COSA and governs all uses of electronic signatures and electronic records used to conduct official City business.

Policy

Electronic signatures, an automated function that replaces a handwritten signature with a system generated signature statement, and electronic records can be utilized as a means for authentication of documents, computer generated documents and/or electronic entries. System generated electronic signatures are considered legally binding as a means to identify the author of medical record entries and confirm that the contents are what the author intended. City departments and staff will be allowed to utilize electronic signature in accordance with this directive and City, State, and Federal regulations regarding such.

Policy Applies To

☐ External & Internal Applicants

☒ Current Temporary Employees

☒ Current Full-Time Employees

☐ Current Volunteers

☒ Current Part-Time Employees

☒ Current Grant-Funded Employees

☒ Current Paid and Unpaid Interns

☒ Police and Fire Academy Trainees

☒ Uniformed Employees Under Collective Bargaining Agreements

☒ Current Contract Employees

Definitions

<u>Digital Signature</u>	An electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature.
<u>Electronic</u>	Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
<u>Electronic Record</u>	A record created, generated, sent, communicated, received, or stored by electronic means.
<u>Electronic Signature</u>	An electronic sound, symbol, or process attached to, or logically associated with, a record and executed or adopted by a person with the intent to sign the record.
<u>Record</u>	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. Record definitions for the City of San Antonio are contained in COSA Administrative Directive 1.34.
<u>Transaction</u>	An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs. Note: As used in this policy, the term "transaction" is intended to refer to the sending or acceptance of electronic records and electronic signatures by City staff, to and from other organizations or individuals.

Policy Guidelines

<u>General Guidelines</u>	<p>A. Use of Electronic Records and Electronic Signatures</p> <ol style="list-style-type: none"> 1. Where policies, laws, regulations, and rules require a signature, that requirement is met if the document contains an electronic signature. 2. Where policies, laws, regulations, and rules require a written document, that requirement is met if the document is an electronic record. 3. Each party to a transaction must agree to conduct the transaction electronically in order for the electronic transaction to be valid. Consent may be implied from the circumstances, except with respect to the electronic records used to deliver information for which consumers are otherwise entitled by law to receive in paper form (i.e., hard copy). 4. If a law prohibits a transaction from occurring electronically, the transaction must occur in the manner specified by law. 5. If a law requires an electronic signature to contain specific elements, the electronic signature must contain the elements specified by law. 6. If a law requires that a record be retained, that requirement is satisfied by retaining an electronic record of the information in a record that accurately reflects the information set forth in the original record and shall remain accessible for later reference. When the requirements for
----------------------------------	--

retention require an original form, retention by an “electronic form” shall provide and satisfy the retention requirement.

B. Procedures, Forms, Guidelines, and Resources

1. Procedures for electronic signatures can be found under the *Texas Uniform Electronic Transactions Act* (http://www.dir.state.tx.us/standards/UETA_Guideline.htm).
2. United States governance can be found in *18 USC 2510, Electronic Communications Privacy Act* (http://www.usdoj.gov/criminal/cybercrime/wiretap2510_2522.htm).
3. Record Management for COSA is established by Local Government Code: 201 through 205. The Texas State Legislature requires local governments to establish a records program by Ordinance.
 - a. City of San Antonio adopted Ordinance 70508 and 72054.
 - b. Ordinance 70508 (November 2, 1989) names the City Clerk as the City’s Records Management Officer.
 - c. Ordinance 72054 (August 9, 1990) establishes the City’s Records Management Program.
 - d. The charter of the City of San Antonio mandates that the City Clerk shall keep the records of the Council and of the City.
 - e. “Pursuant to Article II, Section 10 of the Charter for the City of San Antonio the City Clerk shall keep the records of the Council and of the City. Pursuant to City Ordinance 72054 which establishes the City’s records management program in compliance with the Local Government Records Act and reaffirms City Ordinance 70508 naming the City Clerk as the City’s Records Management Officer, both ordinances filed with the Texas State Library and Archives Commission, the Records Management Officer shall develop policies and procedures in the administration of the City’s records management program. This policy does not supersede any local, state or federal laws regarding records management, confidentiality, information dissemination or standards of conduct.”

C. Electronic Transactions and Signed Records

1. Electronic Records

- a. The Uniform Electronic Transactions Act (UETA) was enacted into law in Texas by the 77th Legislature (Senate Bill 393) in May 2001, and became effective on January 1, 2002. UETA provides definitions for several key terms that pertain to this policy. These terms are listed in the “Definition” section of this directive.

2. Electronic Signatures

- a. Texas law (Government Code, Section 2054.060, <http://tlo2.tlc.state.tx.us/statutes/docs/GV/content/htm/gv.010.00.002054.00.htm>) provides a definition for the term “digital signature,” which is sometimes used interchangeably with “electronic

signature” (see Section II, C, 3).

- b. The State of Texas Guidelines for the Management of Electronic Transactions and Signed Records is located at:

http://www.dir.state.tx.us/standards/UETA_Guideline.htm.

3. Digital Signature

- a. It should be noted that the term digital signature is now generally accepted as referring to a particular type of electronic signature that is created by cryptographic means involving the use of two mathematically related keys (a public and private key pair, often referred to as Public Key Infrastructure or PKI).
- b. Both the definition of “electronic signature” in the UETA and the definition of “digital signature” in Section 2054.060, Government Code, incorporate the concept of ‘intent’ (which is, the ‘intent’ of a person to sign an electronic record).
- c. Electronic signatures may be accomplished by several different technologies, such as Personal Identification Number (PIN), digital signatures, smart cards, and biometrics. If additional technology-specific records management guidance is necessary, ITSD will work with departments to develop it.
- d. Electronic signatures often involve the creation of new records in addition to the electronic record that has been signed. These new records must also be retained as a part of a City entity’s records retention program.

4. Trustworthy Records

- a. Trustworthy records are *reliable*, *authentic*, have maintained their *integrity*, and are *usable*. Each of these terms is discussed below.
- b. The degree of effort a City agency expends on creating or maintaining trustworthy records depends on the agency’s business needs or perception of risk. Transactions that are critical to the City’s business needs may require a greater assurance level that they are reliable, authentic, maintain integrity, and are more usable than less critical transactions. Notwithstanding, this directive does not apply to the issue of whether an electronic record is usable in a legal proceeding.
- c. Under Texas Business and Commerce Code, Section 43.013, evidence of a record or signature may not be excluded in a legal proceeding solely because it is in electronic form. Consequently, for guidance on whether signed electronic records are useable or trustworthy for a particular legal purpose or in a legal proceeding, consult legal counsel.

5. Reliable Records

- a. Reliable records are those whose content can be trusted as a full and accurate representation of the transactions, activities, or facts to which they attest and can be depended upon in the course of

subsequent transactions or activities.

6. Authentic Records

- a. Authentic records are those that are proven to be what they are purported to be, and to have been created or sent by the person who purports to have created and sent them (i.e., non-repudiation).
- b. To demonstrate the authenticity of records, City entities should document and implement policies and procedures that control the creation, transmission, receipt, and maintenance of records. These policies and procedures should ensure that record creators have been authorized and identified, and that records have been protected against unauthorized addition, deletion, and alteration.

7. Records That Have Integrity

- a. Records must be protected against alteration without appropriate permission. Records management policies and procedures should specify what, if any, additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation or addition to a record made after it is complete should be explicitly indicated as an annotation or addition.
- b. The structural integrity of records must be maintained. The physical and logical format of the record and the relationships among the data elements comprising the record should remain intact. Failure to maintain a record's structural integrity may impair its reliability and authenticity.

8. Usable Records

- a. Usable records are those that can be located, retrieved, presented, and interpreted. In any subsequent retrieval and use, the record should be capable of being directly connected to the business activity or transaction that produced it. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

9. Ensuring Trustworthy Electronically Signed Records

- a. To create trustworthy records with electronic signatures:
 - (1) Create and maintain documentation of the systems used to create the records that contain electronic signatures.
 - (2) Ensure that the records that include electronic signatures are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction.
 - (3) Implement standard operating procedures (SOP) for the creation, use, management, and preservation of records that contain electronic signatures and maintain adequate written documentation of those procedures.

	<p>(4) Create and maintain records according to documented SOPs.</p> <p>(5) Train all necessary staff in the SOPs.</p> <p>D. Enforcement</p> <ol style="list-style-type: none"> 1. The CTO, shall have authority to interpret and apply this directive. This directive does not supersede any Ordinance or Administrative Directive pertaining to Records Management as outlined in Administrative Directive 1.34 Paper, Microfilm, and Electronic Records Management. Interpretation in applying this policy for Records Management will be in conjunction with the City Clerk's office. 2. This directive may be modified or amended at any time, if it has been through a formal review and approval process. The CTO shall provide notice of any such modifications or amendments and will post the current version in a publicized location where all authorized users of COSA may access it.
--	--

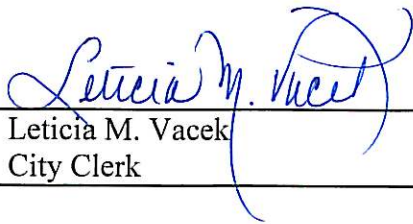
Roles & Responsibilities

<u>Information Technology Services Department</u>	<p>A. Review this directive annually, at a minimum, for both consistency and accuracy</p> <p>B. The CTO, shall have authority to interpret and apply this directive.</p> <p>C. Modify or amend this directive at any time pending formal review and approval as defined in <i>AD 7.5A Establishing IT-Related Directives</i></p> <p>D. Provide adequate notice of any such modifications or amendments</p> <p>E. Ensure the current version of this directive is posted in a public location accessible to all authorized City personnel</p>
<u>Departments</u>	<p>A. Responsible for any disciplinary action taken against employees who violate this directive</p> <p>B. Document and implement policies and procedures that control the creation, transmission, receipt, and maintenance of records</p> <p>C. Train all necessary staff on departmental SOPs</p>
<u>Human Resources</u>	<p>A. Provide guidance, as required, to City departments regarding appropriate disciplinary action to be taken against employees who violate this directive</p>

Attachments

<u>N/A</u>	
-------------------	--

Information and/or clarification may be obtained by contacting the City Clerk at 207-7253 or the Information Technology Services Department (ITSD) at 207-8301.


Leticia M. Vacek
City Clerk

12/11/09

Date


Approved by:


Hugh Miller
Information Technology Services Department, CTO/Director

11/19/09

Date

Approved by:


Richard J. Varn
Chief Information Officer (CIO)

1/6/2010

Date

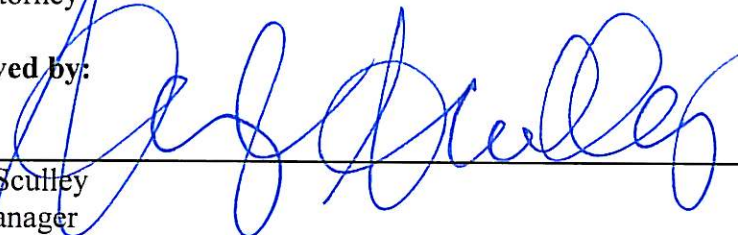
Approved by:


Michael D. Bernard
City Attorney

3/11/2010

Date

Approved by:


Sheryl Sculley
City Manager

3-11-2010

Date